

守护您的重要数据和数字资产

苏黎世中国网络安全保险2020版

对于大多数机构或企业而言，遭遇具有严重破坏性网络攻击的风险是不可避免的。最近，银行木马恶意软件程序“Emotet”卷土重来，让人们重温勒索病毒“NotPetya”带来的教训，并再次展现了恶意软件是如何以惊人的速度在全球蔓延，渗透网络，劫持并加密关键数据，最终造成运营及供应链的中断，产生巨大损失。



全面的保险保障助您防范网络安全风险



苏黎世中国网络安全保险2020版保单的设计简洁且清晰。我们扩展了营业中断收入损失的相关保障，减少并进一步明确除外责任，并对可选批单条款进行了更新。我们希望通过提供有效的扩展条款来更好地满足客户对保险保障的定制需求。此外，我们还简化了术语，使之符合市场标准。

根据波耐蒙研究所发布的《2020年数据泄露成本报告》所示，目前单次数据泄露事件的平均损失为386万美元¹。该研究预估每条丢失或被盗的记录的平均成本为146美元，而那些包含客户PII的被盗记录的平均成本为150美元。因此若一个企业遭遇了严重的数据泄露或盗窃，就可以用该平均成本乘以可能丢失的记录数量，测算得出当次数据泄露事件的总成本。除可量化的损失以外，客户信任度的丢失、对企业形象的负面影响以及企业未来生存发展的压力，这些无形资产的损失又该如何估算呢？

* 波耐蒙研究所《2020年数据泄露成本报告》，该报告由IBM Security赞助发布。
<https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf>



主要保障内容



责任保障

- 安全和隐私责任
- 监管调查诉讼抗辩费用
- 与支付卡产业联盟数据安全标准 (PCI-DSS) 和欧盟《通用数据保护法案》(GDPR) 相关的民事罚款和处罚
- 媒体责任

第一方保障

- 事故响应费用, 包括: 司法鉴证调查费用, 法律和公关费用, 信用和身份监控成本, 身份恢复和身份盗窃保险费用, 呼叫中心成本
- 营业中断收入损失、连带营业收入损失 (即, 由于供应商的网络安全事件而导致的被保险人的损失) 和额外费用
- 数字资产重置费用
- 网络勒索威胁和赎金与报酬支付
- 操作失误导致的营业中断收入损失及连带营业中断收入损失
- 声誉损失
- 社会工程学犯罪相关损失
- 索赔规避费用

保障亮点

- 保障范围增加硬件失效替换费用、善意补偿费用和电话盗用费用批单
- 保障范围中服务中断包括自愿关停和监管关停
- 保障范围增加服务供应商定义扩展至包括指定的业务流程外包商的批单
- 保障范围涵盖数据采集不当行为
- 保障范围覆盖欧盟《通用数据保护法案》(GDPR)
- 被保险人的定义扩大到包括临时雇员、志愿者或实习生
- 修改额外费用的定义, 纳入会计鉴证服务相关费用
- 硬件改善费用
- 计算机系统定义扩大, 包括工业控制系统(ICS)和自带办公设备 (BYOD)
- 取消对保险服务供应商的限制, 客户可自主选择保险事故后的服务供应商 (具体参见条款和条件)



苏黎世中国网络安全保险支持性服务



网络安全风险工程服务

有效且强大的网络安全系统需要由人员、流程和技术三个支柱支撑。苏黎世网络安全风险工程服务可以帮助您的企业建立起这三大支柱，并协助您制定和维护有效的网络安全计划。



• 网络安全评估

- 苏黎世网络风险工程师可通过进行网络风险评估帮助您了解潜在的网络安全风险:
 - 分析您的核心业务流程中潜在的网络安全风险
- 识别您的控制设置中存在的弱点
- 以行业同行为基准, 衡量您的网络态势的成熟度
- 确定并优先考虑改善网络安全的对策



• 人员

- 董事会和高管培训
- 网络用户安全意识培训, 包括网络钓鱼、社会工程、密码标准与管理以及商业电子邮件泄露等内容
- 信息安全管理团队培训
- 雇佣政策安全指南
- 用户访问管理 (例如: 用户、供应商、特权用户和远程用户)



• 流程

- 网络安全策略
- 安全能力规划
- 政策和程序开发, 包括但不限于许可使用、资产管理、漏洞和补丁程序管理、风险评估、供应商管理、事件响应和灾后恢复
- 网络安全管理度量



• 技术

- 与各领域的主要安全技术顾问及服务供应商合作, 提供专业的技术建议



苏黎世中国的服务能力

苏黎世中国已成功建立了本地的专家服务团队，精心挑选了各领域的优质服务机构，旨在为客户提供专业、响应及时且可用母语交流的本地专家服务，其中包括：

- IT鉴证专家和顾问
- 数据保护和网络安全方面的法律专家
- 公关顾问
- 法务会计师
- 从事网络安全保险理赔的专业保险公估人

所有服务机构均凭借雄厚的专业实力、高品质的服务和已建立的服务网络由苏黎世中国甄选而出，定能给予客户在应对重大网络安全事件时的信心和支持。

为选择苏黎世网络安全保险的组织提供的服务包括但不限于：

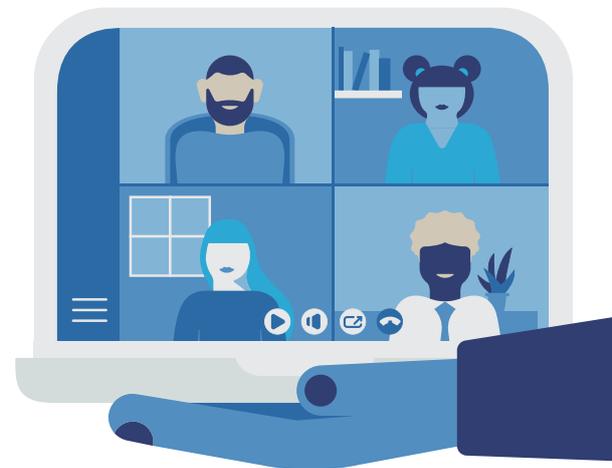
- 远程和现场漏洞检测
- 网络安全综合评估
- 加强网络安全意识的员工培训
- 全年网络威胁警告邮件通知
- 鉴证服务和事故评估
- 法律咨询和辩护
- 网络安全合规性检查
- 公共关系处置

为什么选择苏黎世？



苏黎世保险致力于通过专业的保险技术和丰富的行业经验为客户所珍爱的一切提供最好的保险保障。以客户为中心，且不断超越客户的期望是我们的核心价值理念。150多年来，我们竭诚为客户提供可靠与高效益的保险服务，并凭借专业性、技术性和稳定性赢得客户的长期信赖。

苏黎世保险在200多个国家和地区管理着超过7,800个全球保险业务项目，具有卓越的全球保险业务能力。



苏黎世保险:网络安全保险的首选

一直以来,苏黎世保险被誉为保险新兴领域的思想先驱。苏黎世保险是世界上最早推出网络安全保险产品的保险公司之一,且在北美、欧洲、亚太和拉丁美洲地区业务增长迅速。苏黎世中国在2013年11月推出国内第一个网络安全保险产品。

随着互联网与现实世界的紧密结合,网络风险的性质正在发生根本性的变化。我们认为,在不断变化的网络安全环境下,网络空间作为经济增长和社会发展动力的可靠性正面临严峻挑战,为了保护网络空间的安全性和可靠性,政府、私营企业和社会团体等多方利益攸关者必须通力合作。

我们为客户提供以下支持:

- 加强的保险保障范围;
- 简洁明了的全球一致的保单语言同时又保证本地化以反映当地各项法律要求和法律风险;
- 改善条款语言确定性和保障适用性;
- 承保、理赔、风险工程和合规方面的专业团队;
- 我们会密切持续关注全球法律监管规定的制订、诉讼的发展和新兴风险的出现,不断审视我们的保险产品,以提供应对方案;
- 遍布全球的理赔专家随时待命,提供客户所需的帮助。

苏黎世财产保险(中国)有限公司

地址: 上海市中国(上海)自由贸易试验区世纪大道100号上海环球金融中心32楼
北京市朝阳区曙光西里甲5号院21号楼凤凰置地广场F座写字楼第6层606室
广东省广州市海珠区琶洲大道78号1901室(部位:自编01)

邮编:200120
邮编:100028
邮编:510308



中国官网: www.zurich.com.cn

客服热线: 400 615 5156

联系电话: 上海分公司 021-2089 5500
北京分公司 010-8454 7799
广东分公司 020-3809 4863

微信公众号: Zurich-China



苏黎世保险集团(Zurich)是一家领先的多险种保险公司,为200多个国家和地区的个人和企业客户提供服务。目前,集团拥有约60000名员工,总部位于瑞士苏黎世。成立于150年前的苏黎世保险集团正在改变保险业,我们在为客户提供全面保险服务的同时还关注可持续发展,并逐步增加提供如改善民生福祉和增强气候适应性等方面的保障服务。作为财富世界500强的企业,苏黎世保险集团拥有雄厚的财务实力,并获得国际权威评级机构标准普尔“AA”、穆迪Aa3及AM Best“A+”的评级。

*本资料内容仅供参考,不构成保险合同的任何组成部分,
苏黎世财产保险(中国)有限公司保留在法律允许范围内的最终解释权。

